cpl.thalesgroup.com

THALES

YES BANK Secures Mobile Payment Transactions with Thales Luna HSMs

YES BANK is a frontrunner in developing and offering India's national Unified Payment Infrastructure (UPI) to its mobile banking customers. The Bank chose to implement the Thales Luna Network Hardware Security Module (HSM) to encrypt sensitive data and provide a hardware vault for private keys used in mobile payment transactions.

The Organization

YES BANK, India's fifth-largest private-sector bank, was founded to establish a high-quality, customer-centric, service-driven private bank catering to the future businesses of India. The bank has adopted international best practices, the highest standards of service quality and operational excellence, and offers comprehensive banking and financial solutions to its valued customers with over 900 branches and 1,710+ ATMs across the country.

The Business Need

The National Payments Corporation of India (NPCI) is a nationwide organization overseeing all retail payments systems. NPCI set forth a new initiative of implementing "Unified Payment Interface" (UPI) to simplify and standardize mobile payments through users' smartphones. YES BANK is a frontrunner in deploying UPI to their customers, allowing account holders to send and receive money from their smartphones using a single identifier – mobile telephone number, virtual payment address, or a government-issued ID, like an Aadhaar number – without entering any bank account information.

The UPI must be secure, while also being simple for customers to use, scalable to billions of users as mobile payment adoption grows in the future, and built so that future innovations can be integrated into the application functionality without changing the user interface.

Challenge

When the National Payments Corporation of India (NPCI) set forth a new initiative for smartphone payment transactions, YES BANK was one of the first to develop and offer the technology to customers. But they required additional security measures to protect sensitive data used in financial transactions.

Solution

YES BANK chose the Luna Network HSM to provide strong end-to-end data security and encryption to protect user credential confidentiality and the private keys responsible for digital signing in the UPI mobile app.

Benefit

The Luna Network HSM establishes a secure root of trust for financial transactions throughout the UPI payment process, as well as enabling YES BANK to leverage the new technology to add robust encryption and key vaulting capabilities to other programs and projects.

YES BANK

" With a widespread network of over 900 branches and 1,710+ ATMs pan India, we're committed to taking a customer-centric approach to our banking services. The Unified Payments Interface offers clients revolutionary convenience when it comes to banking and payments, and we want to ensure the highest levels of security for users of the platform. We're thrilled to integrate Thales' industry-leading Luna HSM technology into the UPI application to support this initiative."

– Anup Purohit, Chief Information Officer at YES BANK

The Solution

YES BANK had several capabilities and technical specifications required in an HSM, including:

- Generate private keys and certificates to send to NPCI
- Develop and implement robust encryption and private key security that is required to minimize the risks during transactions as required by the UPI security architecture
- Secure the UPI RSA-2048 Private Keys within the tamper-proof, FIPS 140-2 certified memory boundary of HSM
- Provide API to perform RSA 2048 decryption, base 64 decoding and re-encryption using double DES symmetric key of issuer for sensitive credential contained in incoming UPI message block
- Provide support for multithreaded application processing financial transactions

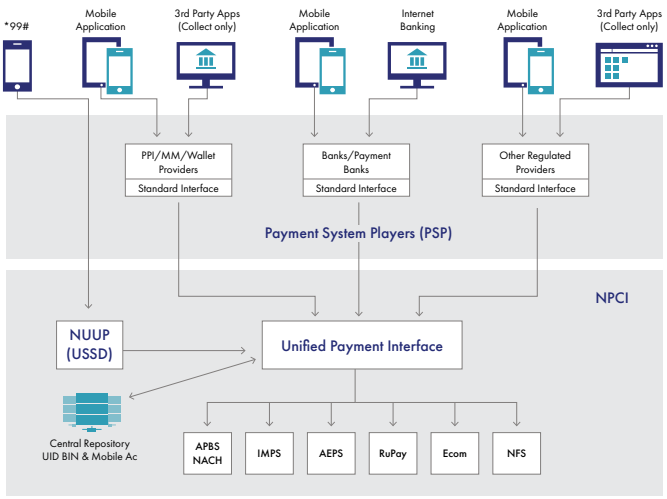
To accomplish these goals, YES BANK selected the Luna Network HSM as the root of trust for encryption keys used in its new UPI payment application.

YES BANK evaluated the sensitivity of information being transmitted during each payment transaction and classified data as:

- Non-Sensitive: can be stored and transmitted in cleartext
- Private: may be stored and transmitted in encrypted form, and ideally encryption keys would be stored in an HSM
- Sensitive: must always be transported in encrypted form, never stored, and decryption keys must reside in a tamper-resistant HSM.

Based on these classifications of data, it was clear that YES BANK required solutions for encryption, as well as an HSM to act as a vault for encryption keys.

The Luna Network HSM is the most trusted hardware security module on the market, and can be easily integrated into a wide range of applications to secure the crypto key lifecycle, and act a root of trust for the entire encryption infrastructure. Unlike other methods of key storage which move keys outside of the HSM into a "trusted layer," the keys-in-hardware approach protects the entire key lifecycle within the FIPS 140-2 validated confines of the Luna Network HSM appliance.



The Benefits

Since implementing the Luna Network HSM, YES BANK has achieved their goals, as well as enjoyed several other benefits.

UPI Security and Compliance with NPCI Standards. The Luna Network HSM provides strong end-to-end data security and encryption to protect user credential confidentiality and the private keys responsible for digital signing, thus establishing a secure root of trust for financial transactions throughout the UPI payment process. The Luna Network HSM also complies with the standards set forth by NPCI, including FIPS 140-2 certification.

Multi-purpose Technology. Since the Luna Network HSM is tightly integrated with the UPI application, not only it is securing the private key responsible for the decryption of user credentials, but the same HSM can be utilized for multiple purposes during the workflow of any UPI transaction. These may be securing private key responsible for SSL handshake to establish the HTTPS session, or securing private key of an UPI participant responsible for digitally signing the XML messages.

Future Capabilities. The Bank has begun planning to leverage the Luna Network HSMs for other projects and applications that will benefit from robust encryption and key management capabilities, such as authentication user agency, Permanent Account Numbers (PAN) verification, and document signing for bank statements and customer communications, as well as use with the e-KYC customer identification process and NPCI's National Automated Clearing House (NACH).

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

> thalesgroup.com <

Americas – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel: +1 888 343 5773 or +1 512 257 3900 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: apacsales.cpl@thalesgroup.com
Europe, Middle East, Africa – 350 Longwater Ave, Green Park, Reading, Berkshire, UK RG2 6GF • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com